ALGEBRA

SECOND EDITION

SAUNDERS MacLANE

GARRETT BIRKHOFF

ALGEBRA

SECOND EDITION

SAUNDERS MacLANE

Max Mason Distinguished Service Professor of Mathematics
The University of Chicago

GARRETT BIRKHOFF

Putnam Professor of Pure and Applied Mathematics
Harvard University

MACMILLAN PUBLISHING CO., INC.

New York

COLLIER MACMILLAN PUBLISHERS

London

Copyright © 1979, Macmillan Publishing Co., Inc.

Printed in the United States of America

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the Publisher.

Earlier edition Copyright © 1967 by Macmillan Publishing Co., Inc.

Macmillan Publishing Co., Inc.
866 Third Avenue, New York, New York 10022

Collier Macmillan Canada, Ltd.

Library of Congress Cataloging in Publication Data

Mac Lane, Saunders, (date)
Algebra.

Includes bibliographies and index.
1. Algebra, Abstract. I. Birkhoff, Garrett, (date) joint author, II. Title.
QA162.M33 1979 512'.02 78-6946
ISBN 0-02-374310-7

Printing: 1 2 3 4 5 6 7 8 Year: 9 0 1 2 3 4 5

Preface to the Second Edition

THIS BOOK aims to present modern algebra from the beginning, for undergraduates or graduates, by covering the standard materials in a way which combines the use of algebraic manipulations and axiomatic methods with the striking general ideas which have developed in recent decades.

The "modern" approach to algebra rests on the use of axioms for groups, rings, fields, lattices, and vector spaces as a means to understanding algebraic manipulations. This modern approach became generally accepted on the graduate level shortly after the publication in 1930 and 1931 of Van der Waerden's now classic *Moderne Algebra*.† In the 1940s, other books, including our own *A Survey of Modern Algebra*,† popularized this approach on the undergraduate level, emphasizing the central role of vector spaces. In the succeeding decades, algebra has continued to develop vigorously, both in the United States and, much influenced by Bourbaki, in France. This development has to some extent reshaped the conceptual organization of mathematics, for example, in the emphasis on the (homo-) morphisms of each type of algebra, and the consequent use of categories and universal constructions.

Our book is organized around this continued development. For example, the axioms used to describe a vector space with scalars from a field apply also when the scalars are elements of a ring, and thus define a module over that ring. This notion of a module now plays a central role in many parts of algebra and in its applications to topology and differential geometry. Constructions on algebraic systems are often described as functors on the appropriate categories: an adjoint functor, when present, is of central utility. Fortunately, these adjoints can be described in elementary terms as *universals*: The construction of a new algebraic object which solves a specific problem in a universal way, so that every other solution is obtained from this one by a unique morphism.

Our presentation starts with integers, groups, rings, fields, modules, and vector spaces. The integers are constructed from the natural numbers so as to provide the universal enlargement of the natural numbers which will allow subtraction. For groups, the projection of a group onto its quotient group provides the universal homomorphism which "kills" the corresponding subgroup. This one property provides all the necessary information about the behavior of quotient groups. The extension of a ring to a ring of polynomials in an indeterminate x is the universal way of adding one new element to a

†See the Bibliography.

ring. The construction of a vector space V with a given basis X is universal in the sense that every linear transformation on V is completely determined by its values on the basis X.

The next chapters treat linear algebra, including tensor products. Proofs of the existence of eigenvalues and eigenvectors for linear transformations use the special properties of the real and complex fields, as developed in Chapter VIII. Up to this point the chapters follow in a natural sequence; thereafter the chapters are largely independent (a second chapter on group theory, lattice theory, categories, and multilinear algebra). This is intended to allow considerable latitude in the development of a course based on selected topics.

The treatment of many of these topics in the first edition has been simplified—and clarified—in this second edition. The material on universal constructions, formerly introduced at the end of the first chapter, has now been assembled in Chapter IV, at a point where there are at hand many more effective examples of these constructions. A great many points in the exposition have been clarified, for instance in a simpler construction of the integers, a more elementary description of polynomials, and a more direct treatment of dual spaces. The chapter on special fields now includes power series fields and a treatment of the p-adic numbers. There is a wholly new chapter on Galois theory; in exchange, the chapter on affine geometry has been dropped. New exercises have been added and some old slips have been excised.

The effective completion of any book depends on the help of many people; it is a pleasure to acknowledge that help for this second edition. A number of readers pointed out to us errors and possible improvements in the published version. They include Dominique Bernaroli, J. L. Brenner, R. E. Johnson, T. Karenakaran, E. Klemperer, Ronald Nunke, L. E. Pursell, S. Segal, Jacques Weil, and Charles Wells. We are notably indebted to Frank Gerrish, who thoughtfully provided us with an especially large number of astute comments. Neal Koblitz helped with material on Chapter VIII. Kathy Edwards, Joel Fingerman, Leo Katzenstein, Gaunce Lewis, Miguel LaPlaza, and others examined this revision with care and attention. For typing assistance, we are indebted to Karen McKeown and Janet Mezgolits. Dorothy Mac Lane prepared the index. To all these—and to many others—we express our sincere thanks and appreciation.

SAUNDERS MAC LANE
GARRETT BIRKHOFF

Dune Acres, Indiana
Cambridge, Massachusetts

此为试读，需要完整PDF请访问：www.ertongbook.com

List of Symbols

Symbol	*Usage*	*Meaning*	*Reference*
$\in$	$x \in S$	x is an element of S	I.1
$\notin$	$x \notin S$	x is not an element of S	I.1
$\subset$	$S \subset X$	S is a subset of X	I.1
	$S \subset G$	S is a subgroup of G	II.4
$\varnothing$	$\varnothing$	The empty set	I.1
$\{\ \}$	$\{x \mid —\}$	All x such that	I.1
$\cap$	$S \cap T$	Intersection of S and T	I.1
$\cup$	$S \cup T$	Union of S and T	I.1
$(\ )$	(k, m)	Binomial coefficient $(k + m)!/(k!)(m!)$	III
$(\ )$	(x, y)	Ordered pair of x and y	I.3
$\times$	$X \times Y$	Product of X and Y	I.3
$\Rightarrow$	$\cdots \Rightarrow —$	$\cdots$ implies —	I.1
$\Leftrightarrow$	$\cdots \Leftrightarrow —$	$\cdots$ if and only if —	I.1
$\circ$	$f \circ g$	Composite, f following g	I.2
$\rightarrow$	$X \rightarrow Y$	Function on X to Y	I,2
$\dashrightarrow$	$X \dashrightarrow T$	Function to be constructed	IV.1
$\longmapsto$	$x \longmapsto x^2$	Function assigning x^2 to x	I.2
$\cong$	$X \cong Y$	Bijection (isomorphism) X to Y	I.3
	Y^X	All functions on X to Y	IV.8
$\square$	$x \square y$	Binary operation on x, y	I.3
$\vee$	$x \vee y$	Join of x and y	IV.6
$\wedge$	$x \wedge y$	Meet of x and y	IV.6
	$u \wedge v$	Exterior product of u and v	XVI.6
$\leqslant$	$x \leqslant y$	x less than or equal to y	I.6
		x contained in y (in a lattice)	IV.6
$\mid$	$m \mid n$	m divides n	III.8
$\equiv$	$k \equiv m (\text{mod } n)$	k congruent to m, modulo n	I.8
	$f^{\text{‘}}$	Function given by polynomial f	III.7

Symbol	*Usage*	*Meaning*	*Reference*
$\triangleleft$	$N \triangleleft G$	N normal subgroup of G	II.9
:	$[G : S]$	Index of S in G	II.8
/	X/E	Quotient set of X by E	I.9
	G/N	Quotient group of G by N	II.10
	R/A	Quotient ring of R by ideal A	III.3
	A/D	Quotient module	V.4
*	z^*	Conjugate complex number of z	VIII.7
	$f_* S$	Image of S under f	IV.8
	$f^* T$	Inverse image of T under f	IV.8
	V^*	Dual vector space to V	V.7
	t^*	Dual map to t	V.7
	t^*	Adjoint map to t	X.6
$\oplus$	$A \oplus B$	Biproduct of modules A, B	V.6
$\otimes$	$A \otimes B$	Tensor product of A, B	IX.8
$\vert\ \vert$	$\vert a\vert$	Absolute value of a	VIII.1
	$\vert u\vert$	Length of vector u	X.5
	$\vert A\vert$	Determinant of matrix A	IX.2
$\langle\ \rangle$	$\langle u, v\rangle$	Inner product of u, v	X.5
$\perp$	$u \perp v$	u orthogonal to v	X.5
∞	∞	Infinite (characteristic)	III.1
op	G^{op}	Opposite group	II.2
	R^{op}	Opposite ring	III.2
	$\mathbf{X}^{\mathrm{op}}$	Opposite category	XV.1

Standard Abbreviations	*Meaning*	*Reference*
Aut (G)	Automorphisms of G	II.1
Bilin $(A, B; C)$	Bilinear functions $A \times B \to C$	IX.10
End (A)	Endomorphisms of A	II.2, V.2
hom (X, Y)	Morphisms of X to Y	IV.2, XV.1
Hom (A, B)	Group of morphisms, A to B	V.2
$GL(n, F)$	General linear group	VII.6, IX.3
O_n	Orthogonal group	X.7
$SL(n, K)$	Special linear group	IX.3
dim V	Dimension of V	VI.2
rank A	Rank of A	VI.3, VII.5

Letters with Fixed Meanings	*Meaning*	*Reference*
A_n	Alternating group	II.6
C	Field of complex numbers	VIII.7
N	Set of natural numbers	I.4
Q	Field of rational numbers	III.5
R	Field of real numbers	VIII.5
S_n	Symmetric group	II.6
Z	Ring of integers	I.7
n	$\{1, 2, \cdots, n\}$	I.7
Δ_n	Dihedral group	II.5
δ_{ij}	Kronecker delta	VI.4
ε_i	Unit vectors	V.5

Contents

此为试读，需要完整PDF请访问：www.ertongbook.com

CHAPTER I

Sets, Functions, and Integers

ALGEBRA starts as the art of manipulating sums, products, and powers of numbers. The rules for these manipulations hold for all numbers, so the manipulations may be carried out with letters standing for the numbers. It then appears that the same rules hold for various different sorts of numbers, rational, real, or complex, and that the rules for multiplication even apply to things such as transformations which are not numbers at all. An algebraic system, as we will study it, is thus a set of elements of any sort on which functions such as addition and multiplication operate, provided only that these operations satisfy certain basic rules. The rules for multiplication and inverse are the axioms for a "group", those for addition, subtraction, and multiplication are the axioms for a "ring", and the functions mapping one system to another are the "morphisms". This chapter starts with the necessary ideas about sets, functions, and relations. Then the natural numbers are used to construct the integers and the integers modulo n, with their addition and multiplication. This serves as an introduction to the notion of a morphism from one algebraic system to another.

Many developments in algebra depend vitally upon defining the right concept. When our presentation reaches any definition, the term being defined is put in italics, as *group, ring, field*, and so on. However, terms little used in the sequel as well as terminology alternative to that selected here are put in quotation marks; thus "range" stands for *codomain* and "onto" for *surjective* (see §2 below).

A reference such as Theorem 3 is to Theorem 3 of the current chapter, while Theorem II.3 is to Theorem 3 of Chapter II. In like manner, Corollary IV.5.2 refers to Corollary 2 of Theorem 5 of Chapter IV, and Equation (VI.11) to Equation (11) of Chapter VI. Within each Chapter, Theorems and Propositions are numbered in a single series. More difficult exercises and sections which may be omitted on first reading are denoted by an asterisk, *.

1. Sets

Intuitively, a "set" is any collection of elements, and a "function" is any rule which assigns to each element of one set a corresponding element of a second set.

Examples of sets abound: The set of all lines in the plane, the set **Q** of all rational numbers, the set **C** of all complex numbers, the set **Z** of all integers (positive, negative, or zero). Sets with only a finite number of different elements may be described by listing all their elements, often indicated by writing these elements between braces. Thus the set of all even integers between 0 and 8, inclusive, may be exhibited as $\{0, 2, 4, 6, 8\}$, while the set of all positive divisors of 6 is the set $\{1, 2, 3, 6\}$. The order in which the elements of a set are listed is irrelevant: $\{1, 3, 6, 2\} = \{1, 2, 3, 6\}$.

More formally, "$x \in S$" stands for "x is an *element* of the set S" or equivalently, "x is a member of the set S" or "x belongs to S". Also, $x \notin S$ means that x is *not* an element of S. Since a set is completely determined by giving its elements, two sets S and T are *equal* if and only if they have the same elements; in symbols:

$$S = T \quad \Leftrightarrow \quad \text{For all } x,\ x \in S \text{ if and only if } x \in T. \tag{1}$$

(Here the two-pointed double arrow "$\Leftrightarrow$" stands for "if and only if".) Also, S is a *subset* of T (or, is *included* in T) when every element of S is an element of T, so that, if $x \in S$, then $x \in T$; in symbols:

$$S \subset T \quad \Leftrightarrow \quad \text{For all } x,\ x \in S \Rightarrow x \in T.$$

(Here, on the right, the one-pointed double arrow "$\Rightarrow$" stands for "implies".) By this definition, $S \subset T$ and $T \subset U$ imply $S \subset U$, while the equality of sets, as defined above, may be rewritten as

$$S = T \quad \Leftrightarrow \quad S \subset T \text{ and } T \subset S.$$

A set S is *empty* if it has no elements. By the equality rule (1), any two empty sets are equal. Hence, we speak of *the* empty set, written $\varnothing$. It is also called the *null set* or the *void set;* it is a subset of every set. Also, S is a *proper subset* of a set U when $S \subset U$ but $S \neq \varnothing$ and $S \neq U$.

A particular subset of a given set U is often described as the set of all those elements x in U which have a specified property. Thus the subset of those complex numbers z such that $z^2 = -1$ is written $\{z \mid z \in \mathbf{C} \text{ and } z^2 = -1\}$, while the formulas

$$E = \{x \mid x \in \mathbf{Z} \text{ and } x = 2y \text{ for some } y \in \mathbf{Z}\}, \qquad N = \{x \mid x \in \mathbf{Z} \text{ and } x > 0\}$$

describe the set E of all even integers and the set N of all nonnegative integers, respectively. Different properties may describe the same subset; thus

$$\{n \mid n \in \mathbf{Z} \text{ and } 0 < n < 1\} \qquad \text{and} \qquad \{n \mid n \in \mathbf{Z} \text{ and } n^2 = -1\}$$

both describe the empty set $\varnothing$.

Next we consider the operations of intersection and union on sets. If R and S are given sets, their *intersection* $R \cap S$ is the set of all elements common to R and S:

$$R \cap S = \{x | x \in R \text{ and } x \in S\},$$

while their *union* $R \cup S$ is the set of all elements which belong either to R or to S (or to both):

$$R \cup S = \{x | x \in R \text{ or } x \in S\}.$$

These definitions may be stated thus:

$$x \in (R \cap S) \quad \Leftrightarrow \quad x \in R \text{ and } x \in S,$$

$$x \in (R \cup S) \quad \Leftrightarrow \quad x \in R \text{ or } x \in S.$$

This display correlates the operations of intersection and union with the logical connectives "and" and "or". The corresponding correlate of "not" is the operation of "complement": If S is a subset of U, the *complement* S' of S *in* U is the set of all those elements of U which do not belong to S:

$$S' = \{x | x \in U \text{ and } x \notin S\}.$$

For example, for the sets E and N above, $E \cap N$ is the set of even nonnegative integers, $E \cup N$ the set of all integers except the negative odd ones, while the complement E' of E in $\mathbf{Z}$ is the set of all odd integers.

The operations of intersection, union, and complement satisfy various "identities", valid for arbitrary sets. A sample such identity is

$$R \cap (S \cup T) = (R \cap S) \cup (R \cap T), \tag{2}$$

valid for any three sets R, S, and T. (This equation states that the operation "intersection" is distributive over the operation "union".) To prove this statement, consider any element x. By the definitions of $\cap$ and $\cup$ above,

$$\begin{aligned} x \in [R \cap (S \cup T)] \quad &\Leftrightarrow \quad x \in R \text{ and } x \in S \cup T \\ &\Leftrightarrow \quad x \in R \text{ and } (x \in S \text{ or } x \in T). \end{aligned}$$

For similar reasons,

$$x \in [(R \cap S) \cup (R \cap T)] \Leftrightarrow (x \in R \text{ and } x \in S) \text{ or } (x \in R \text{ and } x \in T).$$

Now, in view of familiar properties of "and" and "or", the two different statements made about x at the right of the two displays above are logically equivalent. Hence, the two sets in question have the same elements and therefore are equal. In other words, this proof reduces property (2) of intersection and union to an exactly corresponding property of the logical connectives "and" and "or".

A similar argument gives another distributive law,

$$R \cup (S \cap T) = (R \cup S) \cap (R \cup T). \tag{3}$$

Other algebraic properties of intersection, union, and complement will be considered in the exercises in §3 below.

Two sets, R and S, are called *disjoint* when $R \cap S = \varnothing$.

Given a set U, the set $P(U)$ of all subsets S of U is called the *power set* of U; thus $P(U) = \{S \mid S \subset U\}$. For example, if U has two elements, it has four different subsets which are the four elements of $P(U)$. Explicitly, $P(\{1, 2\}) = \{\{1, 2\}, \{1\}, \{2\}, \varnothing\}$. Here $\varnothing$ is the empty set (a subset of every set, as above).

EXERCISES

1. For subsets R, S, and T of a set U, establish the following identities:
   (a) $R \cap S = S \cap R, \quad R \cap (S \cap T) = (R \cap S) \cap T.$
   (b) $R \cup S = S \cup R, \quad R \cup (S \cup T) = (R \cup S) \cup T.$
   (c) $(R \cap S)' = R' \cup S', \quad (R \cup S)' = R' \cap S'.$
   (d) $S \cap (S \cup T) = S, \quad S \cup (S \cap T) = S.$
2. Show that any one of the three conditions $S \subset T$, $S \cap T = S$, and $S \cup T = T$ on the sets S and T implies both of the others.
3. For $S \subset U$, show that $S \cap S' = \varnothing$ and $S \cup S' = U$.
4. List the elements of the sets $P(P(\{1\}))$ and $P(P(P(\{1\})))$.
5. Show that a set of n elements has 2^n different subsets.
6. If $m < n$, show that a set of n elements has $(n!)/(n-m)!(m!)$ different subsets of m elements each, where $m! = 1 \cdot 2 \cdots m$.

2. Functions

A *function* f *on* a set S *to* a set T *assigns* to each element s of S an element $f(s) \in T$, as indicated by the notation

$$s \mapsto f(s), \qquad s \in S.$$

The element $f(s)$ may also be written as fs or f_s, without parentheses; it is the *value* of f at the *argument* s. The set S is called the *domain* of f, while T is the *codomain*. The *arrow* notation

$$f : S \to T \qquad \text{or} \qquad S \xrightarrow{f} T$$

indicates that f is a function with domain S and codomain T. A function is often called a "map" or a "transformation".

To describe a particular function, one must specify its domain and its codomain, and write down its effect upon a typical ("variable") element of its domain. Thus the squaring function $f: \mathbf{R} \to \mathbf{R}$ for the set $\mathbf{R}$ of real numbers may be described in any of the following ways: As the function f with $f(x) = x^2$ for any real number x, or as the function $(-)^2$, where — stands for the argument, or as the function which sends each $x \in \mathbf{R}$ to x^2, or as the

此为试读，需要完整PDF请访问：www.ertongbook.com